VASILE MAIEREAN - În căutarea cifrului perfect - Sezonul I -

(din Revista LUMEA nr.5/2012)



















Vasile Maierean

În căutarea cifrului perfect
(Sezonul I)

În anul 1959 avea loc premiera unui film mai puţin obişnuit pentru peisajul cultural al epocii. Se intitula „Secretul cifrului”, avea un scenariu scris de Dumitru Carabăţ după romanul lui Theodor Constantin „La miezul nopţii va cădea o stea” și era regizat de maestrul Lucian Bratu. Filmul descrie acțiunile unui ofițer sub acoperire (cpt. Ulea), aparținând serviciului de contraspionaj românesc, pentru capturarea unui spion german (Tălâmbu), infiltrat într-o unitate de transmisionişti aflată pe linia frontului antihitlerist, având ca misiune sustragerea unui dispozitiv de cifrare al armatei române. Filmul îşi păstrează prospeţimea artistică și astăzi datorită scenariului şi interpretării excelente a unor actori inegalabili precum Emanoil Petruţ, Mihai Mereuţă, Olga Tudorache și Benedict Dabija. Totodată, a rămas de actualitate și tematica: războiul permanent pentru titlul de stăpân absolut al “secretului cifrului”.





Afişe ale filmului „Secretul cifrului”

Întrucât subiectul este extrem de vast şi de fascinant, având o istorie milenară, ne vom rezuma în acest prim Sezon al eseului doar la problema preocupării criptografilor de a crea sisteme de cifrare rezistente și la încercările criptanaliştilor de a le sparge. Lupta permanentă dintre criptografii specializaţi în elaborarea cifrurilor şi criptanaliştii concentrați pe decriptarea lor, constituie motorul “perpetuum mobile” al perfecţionării sistemelor criptologice.

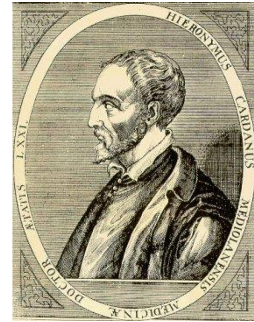
Învăţaţii, care s-au aplecat asupra chestiunilor criptografice, şi-au dat seama că în orice limbă literele au o anumită frecvenţă. Filologii, cercetători specializaţi în analiza structurii limbajelor naturale, au constatat că literele, bigramele, cuvintele şi unele expresii au frecvenţe relativ stabile în limbă. Sistemele criptografice clasice, bazate în general pe substituirea acestor elemente, nu au putut ascunde în totalitate aceste frecvenţe, oferind astfel criptanaliştilor un punct de sprijin. Nume prestigioase ale istoriei criptologiei, precum Alberti, Trimethius, Vigenere, Cardano, Contesa de Lovelace/Augusta Ada Byron/ (primul programator din lume pentru un calculator mecanic- calculatorul lui Charles Babbage), Kerckhoff - pentru a cita doar câteva nume - au marcat momente importante din dezvoltarea criptologiei, elaborând mereu cifruri tot mai complexe.



Blaise de Vigenere



Contesa de Lovelace



Girolamo Cardano

S-a ajuns astfel la sistemele de cifru cu chei aleatoare, considerate indecriptabile, atât din punct de vedere teoretic cât şi practic. Cheile întrebuinţate nu au nici o regulă de obţinere.

Cel mai sofisticat sistem de acest tip este "**sistemul cu cheie aleatoare de unică folosinţă**"**,** creat în 1917, cunoscut în literatura de specialitate sub denumirea de **"ONE-TIME PAD"(OTP)**. In cadrul acestui sistem textul clar al mesajului este criptat cu un cifru de substituţie, supracifrat cu o cheie aleatoare ("pad"*)* la fel de lungă ca şi lungimea mesajului, rezultând un text cifrat aleator. În cazul în care algoritmul este cu certitudine aleator, are lungimea mesajului, nu este refolosit niciodată parţial sau în întregime şi se asigură păstrarea lui într-un secret absolut, cifrul este imposibil de decriptat.

Fiind unicul criptosistem considerat perfect din punct de vedere teoretic din epoca pre-computerului, OTP-ul a fost folosit intens pentru realizarea comunicărilor secrete diplomatice, militare şi de spionaj. Linia fierbinte dintre Moscova şi Washington, stabilită în 1963, după criza cubaneză, a folosit teleimprimatoare protejate cu un sistem OTP. Este cunoscut că spionii KGB au folosit şi încă mai folosesc OTP-ul. Exemplele includ pe colonelul Rudolf Abel, care a fost arestat şi condamnat la începutul anilor 1950 la New York, şi Morris şi Lona Cohen, care au fost arestaţi şi condamnaţi pentru spionaj în Marea Britanie la începutul anilor 1960. În ambele cazuri s-au descoperit cifruri OTP în posesia lor.





Colonelul Rudolf Ivanovici Abel

Spargerea cifrurilor OTP s-a datorat fie nerespectării riguroase a regulilor de criptare, fie refolosirii aceloraşi chei numerice la mesaje diferite sau neparafrazării unor documente originale transmise prin cifru dar şi pătrunderilor secrete efectuate de serviciile de informaţii adverse pentru a intra în posesia cheilor aleatoare. Astfel:

- În anii 1944-45, Serviciul de interceptare-decriptare al armatei americane a reuşit să spargă un sistem OTP folosit de Ministerul de Externe german datorită aleatorismului incomplet, maşina de criptat generând algoritmi predictibili.
- În 1945 Statele Unite au descoperit că mesajele între Canberra şi Moscova erau criptate folosind un OTP utilizat şi pe altă linie de comunicaţii iar unele mesaje includeau documente oficiale;
- Începând cu anii 1940, americanii şi britanicii au fost capabili să spargă unele telegrame, cifrate cu sistemul OTP, ale agenturii sovietice ce acţiona pe teritoriile lor în urma unor erori comise în generarea şi distribuirea materialelor de cifru. O ipoteză este aceea că personalul Centralei din Moscova era atât de precipitat de prezenţa trupelor germane chiar la marginea Moscovei la finele anului 1941 şi debutul anului 1942 încât produceau mai mult decât o copie a aceluiaşi material criptografic. Acest efort uriaş de criptanaliză care a durat câteva decenii (până în 1980), codificat VENONA, a produs o considerabilă cantitate de informaţii, inclusiv despre "spionii atomici" sovietici. Chiar în aceste condiţii, doar un mic procentaj din mesajele interceptate au fost decriptate parţial sau în întregime (câteva mii din mai multe sute de mii).
- Prin declasificarea unor documente secrete ale serviciilor de informații americane s-a aflat că în mod sistematic au avut loc, în toată perioada Războiului Rece, penetrări ale agenților FBI în birourile diplomaților sovietici din Statele Unite, în cursul cărora s-au sustras materiale de cifru, care au fost puse apoi la dispoziţia criptanaliştilor**.**

În paralel cu sistemul OTP, a cărui punere în practică implică eforturi complexe și costisitoare, de care în principiu sunt capabile numai structuri oficiale, s-au dezvoltat și alte sisteme criptografice solide, de mai largă posibilitate a folosirii.

Astfel, activitatea criptografică în care se întrebuințează aceeaşi cheie pentru criptare şi decriptare intră în categoria "criptografiei simetrice" sau "criptografiei cu chei secrete". Un astfel de sistem, folosit în epoca calculatoarelor, este cel denumit **DES (Data Encryption Standard** sau **Standard de Criptare Date*)***, un cifru bloc în care mesajul de criptat este divizat în blocuri de lungimi egale şi fixe. Conform schemei DES, algoritmul folosit la criptare are 72.057.594.037.927.936 chei posibile. Deoarece DES, de-a lungul timpului, devenise vulnerabil din cauza lungimii prea mici a cheii, s-a trecut la utilizarea unui nou sistem intitulat **3DES**, un algoritm care constă în esență în aplicarea de trei ori a DES.

Deși 3DES este un algoritm puternic, el s-a dovedit relativ lent în implementările software, motiv pentru care, următorul pas în această ultrarapidă evoluție, a fost adoptarea unui nou sistem propus, în anul 1997, de doi criptografi belgieni, Joan Daemen și Vincent Rijmen. Acesta a fost denumit de autorii săi **Rijndael**, și este cunoscut în lumea specialiștilor sub titulatura **AES (Advanced Encryption Standard** - în limba engleză, **Standard Avansat de Criptare)**. Criteriile pe baza cărora sistemul AES a fost adjudecat pentru utilizare în cazul informațiilor clasificate, de către guvernul SUA, în iunie 2003, au fost: securitatea (rezistența la atacuri criptanalitice), costurile (eficiența computațională, complexitatea spațială, precum și licențierea liberă și gratuită) și particularitățile algoritmului (flexibilitatea, simplitatea, și ușurința de realizare a implementărilor atât software cât și hardware).

Introducerea şi dezvoltarea computerelor a fost însoţită şi de un alt tip de criptografie, în care utilizatorii au o pereche de chei, una publică şi una privată (secretă), denumit "criptografie asimetrică" sau "criptografie cu chei publice" (**PKE**). Cheia publică se foloseşte pentru criptarea unui mesaj care nu poate fi decriptat decât cu cheia pereche,

cea privată. Matematic, cele două chei sunt legate, însă cheia privată nu poate fi obţinută din cheia publică. O analogie a acestui proces o reprezintă folosirea cutiei poştale: oricine poate pune în cutia poştală un plic dar la plic nu are acces decât posesorul cheii cutiei poştale. În anul 1978, trei cercetători de la Massachusetts Institute of Technology, Ron Rivest, Adi Shamir şi Leonard Adleman, au conceput algoritmul **R.S.A.** (Rivest-Shamir-Adleman), devenit ulterior standard pentru criptografia cu chei publice.



Ronald R Rivest



Leonard Adleman



Adi Shamir

Referitor la rolul criptografiei în lupta împotriva "fraudelor informatice", matematicianul Adi Shamir de la Institutul Weizmann din Tel Aviv, remarcabil criptolog, afirma următoarele: "Inconvenientul informaticii este că nici un ordinator nu este inviolabil. Pentru un specialist este doar o problemă de răbdare şi de timp".

În acest sens, criptologia este chemată să elaboreze sisteme criptografice capabile să garanteze securitatea datelor şi informaţiilor stocate sau transmise în reţelele de calculatoare, acţiune foarte dificilă. În acest sens, următorul episod este semnificativ:

În 1977, Ralph Merkel de la Universitatea Stanford a imaginat un astfel de sistem despre care afirma că "este atât de complicat încât ar trebui cel puţin un milion de ani pentru ca cel mai puternic ordinator să-l decripteze". El i-a cerut lui Adi Shamir să încerce să-l decripteze, spunându-i "Pariez pe 100 de dolari că n-o să reuşeşti". În 1982, Shamir i-a telefonat lui Merkel: "Pregăteşte un cec de 100 de dolari. Copilul tău şi-a dezvăluit secretul". Deci, au fost necesari numai cinci ani şi nu un milion de ani.

Ca rezultat al folosirii algoritmilor foarte lungi pentru criptarea cu chei publice şi a metodelor matematice tot mai complexe pentru găsirea acestor chei, activitatea modernă din domeniu a trecut indubitabil din zona amatorismului, exclusiv în cea a specialiştilor. Cu atât mai justificată rămâne sfidarea continuă creată de posibilitatea ispititoare ca în blindajul sistemelor de criptare, care folosesc factorizarea numerelor mari, să existe o fisură, o cale mai simplă.

Chiar în momentul redactării acestui material, agenţiile de presă informează că un expert german a demonstrat cât de vulnerabile sunt măsurile de securitate care protejează sistemul de comunicaţii mobile (GSM), utilizat în întreaga lume, reuşind să spargă un important algoritm de criptare a convorbirilor pe telefonul mobil. Codul de securitate spart de expertul german este utilizat de peste trei miliarde de oameni din 212 ţări.

După 11 septembrie 2001, NSA (Agenția Națională de Securitate din SUA) a devenit beneficiara unor bugete de zeci de miliarde de dolari, care s-a convenit să fie investite în colectarea şi analiza computerizată a tuturor(!) datelor pe care le pot obţine. Pentru colectarea acestui volum imens de date, NSA a creat programul "Stellar Wind" , care constă în amplasarea de aparatură de înregistrare şi transmisie în toate nodurile de comunicare ale companiilor americane de telecomunicaţii.

În aceste condiții, ultima linie de apărare a utilizatorilor împotriva curiozităţii NSA este, deocamdată, tehnica de criptare AES, majoritatea programelor de e-mail şi a browserelor utilizând-o pentru protejarea datelor sensibile. Așa că, specialiștii NSA şi-au concentrat forţele pe învingerea acestui sistem de criptare care, teoretic, în prezent nu poate

fi spart. Conform publicației americane “Wired“, timpul necesar pentru încercarea tuturor combinaţiilor posibile este mai lung decât vârsta Universului. Ca urmare, NSA a proiectat un nou supercomputer, care va fi construit până în 2018. Amplasat, în centrul său din Oak Ridge, în două hale care vor ocupa 2,4 hectare, acesta va fi capabil să efectueze un quintilion (10 la puterea 30) de operaţii pe secundă şi va folosi, la capacitatea maximă, 200 megawaţi - suficientă energie pentru un oraş cu 200.000 locuitori. Cu ajutorul său, NSA speră să spargă şi actualele standarde de criptare - devenind, astfel, stăpânii absoluţi ai informaţiilor.

Dar, ca în toate domeniile în care mintea omului construiește, și în criptografie apare mereu speranța posibilității ridicării unor noi ultime frontiere. Există cercetări și aplicații care demonstrează că principiile teoriei haosului şi legile fizicii cuantice pot fi folosite în criptografie cu rezultate care întrec orice închipuire.

În ultimii ani, idei noi şi radicale au fost dezvoltate pentru elaborarea unei specii complet noi de criptare, în mod real impenetrabilă, **criptografia cuantică**, în care securitatea metodei se bazează pe principiile pure ale fizicii dar şi pe cercetări care explorează posibilităţi aflate dincolo de aceste legi.

În 2007, o echipă de specialişti ai mai multor institute de cercetări europene, sub coordonarea profesorilor Ursula Gerber şi A.Zeilinger de la Universitatea din Viena, a reuşit să teleporteze date la o distanţă de 144 de kilometri, ceea ce constituie o premisă uluitoare, atât pentru teleportarea cuantică (de tip STAR TREK), cât şi pentru criptografie. Reuşita experimentului s-a datorat unor proprietăţi ale materiei în “lumea” mecanicii cuantice (la nivelul atomilor), în care particulele au un comportament ce sfidează fizica clasică, newtoniană. Albert Einstein, îndoindu-se de existenţa efectelor cuantice, le-a numit ***acţiuni supranaturale la distanţă*** („**Paradoxul EPR**” – Einstein, Podolsky, Rosen, 1935).

1. 

Albert Einstein   Boris Yacovlevich Podolski   Nathan Rosen

Existenţa reală a fenomenului a fost evidenţiată pentru prima oară în 1982, de fizicianul francez Alain Aspect de la Universitatea din Orsay. Acesta, împreună cu colaboratorii săi, au demonstrat că există particule care sunt perechi inseparabile, anumite proprietăţi ale lor (energia, impulsul etc.) conservându-se, indiferent de distanţa la care se găsesc una faţă de alta. Astfel, acţiunile exercitate asupra uneia dintre aceste particule au efect instantaneu asupra perechii sale. Potrivit demonstrației, „proprietățile oricărei particule pot fi transferate către o altă particulă, chiar dacă cele doua părţi se află în colţuri opuse ale galaxiei”.

Criptarea cuantică se realizează în conformitate cu cerințele „principiului incertitudinii” al lui Heisenberg, potrivit căruia nu poţi măsura o informaţie cuantică fără să o perturbi. Orice intenţie de a spiona comunicaţia dintre doi utilizatori produce un “zgomot” uşor de sesizat de către aceştia. Acest principiu este aplicat prin utilizarea de particule cuantice – fotonii. Prin transmiterea succesivă a unor fluxuri de fotoni, cuantificarea lor şi procesarea datelor rezultate în urma acestui proces rezultă cheia criptografică. Deci, „informaţia transmisă prin teleportare cuantică nu poate fi interceptată sau copiată” (fizicianul Ignacio Ciriac, de la Max Planck Institute of Quantum Optics).

La începutul lunii octombrie 2008, a fost pusă în funcţiune prima reţea comercială de comunicaţii securizată prin metoda criptografiei cuantice. Această premieră mondială este rezultatul proiectului european SECOQC (Secure Communication based on Quantum Cryptography), în cadrul căruia, începând din anul 2004, 41 de cercetători din 12 state europene au reuşit să construiască în Austria o reţea de calculatoare ce înglobează o infrastructură care constă în 200 de kilometri de cabluri de fibră optică, cele opt legături intermediare existente folosind şase tehnologii de criptografiere prin metode cuantice.

Se pare însă că deja s-au descoperit o breşă în criptografia cuantică, o echipă de cercetători suedezi găsind o vulnerabilitate care contrazice teza că această metodă ar garanta 100% siguranţa comunicării electronice. Ei au demonstrat că, teoretic, există posibilitatea ca o persoană neautorizată să extragă cheia de criptare, fără să fie detectată.

Criptografia cuantică ar fi putut reprezenta un relativ sfârşit al îndelungatei confruntări dintre criptografi şi criptanalişti, dacă, între timp, nu s-ar fi inventat noi mijloace exotice de generare a mesajelor secrete. De exemplu, la sfârşitul lui 2005, un grup de cercetători europeni au descoperit că unele din principiile „teoriei haosului” ar putea fi folosite pentru secretizarea comunicaţiilor. Ideea de bază este că un mesaj poate fi “îngropat” în interiorul unui semnal haotic – un zgomot de origine solară, meteorologică ş.a. – ca paravan care face mesajul inaccesibil celor care nu pot descompune haosul în elemente componente.

Putem conchide că în epoca actuală domeniul criptologiei se află, în bună măsură, în mâinile fizicienilor şi al matematicienilor dar, cea mai mare parte din ceea ce se întâmplă are loc, fără îndoială, ca întotdeauna, în spatele uşilor închise. Agenţiile guvernamentale păstrează informaţiile despre spargerea de coduri şi despre criptografie sub control strict, ceea ce face extrem de dificilă predicţia dezvoltărilor viitoare din domeniu.

În contextul de expansiune ofensivă a cercetărilor în domeniu, David Kahn, fost preşedinte al Asociaţiei Criptologilor Americani şi al Societăţii de Cifru din New York, profesor la Universitatea Yale, specialist în tehnici de spionaj militar, a emis următoarea opinie: „condiţia ca o ţară să poată fi privită ca o superputere este ca ea să deţină propriile tehnologii nucleare şi spaţiale şi propriul sistem de criptografiere”.

În condițiile existenței unei lumi paralele cu cea în care omenirea evoluează de mii de ani, respectiv **lumea calculatoarelor, lume virtuală indestructibilă, descentralizată, proprietate a tuturor**, criptografia a devenit o armă cu două tăişuri. Ea serveşte la garantarea confidenţialităţii şi permite atribuirea cu certitudine a unei informaţii, unei anumite persoane, la un moment dat. Nu mai este rezervată exclusiv militarilor, ci este la dispoziţia întregii societăţi. De aici rezultă însă și realitatea crudă a fețelor întunecate ale posibilităților nelimitate de aplicare a cunoștințelor criptografice.

Sinistra sectă japoneză AUM, care în 1995 a atacat metroul din Tokyo împrăştiind un gaz mortal, îşi stoca, codificate cu algoritmul RSA, toate fişierele din computere. Poliţiştii care au decriptat conţinutului acestora au putut cunoaşte planurile secrete ale sectei de a acţiona şi pe teritoriul american. De asemenea, autorii atentatului de la World Trade Center, din New York, în 1994, şi din metroul oraşului, în anul următor, dispuneau de PC-uri portabile şi de date codificate.

În consecință, lupta se dă și în planul reglementărilor legale ale domeniului.

În SUA, efortul de legiferare a limitelor activităţilor pe care statul sau persoanele particulare le pot desfăşura în domeniul criptologiei a avut de la început ca argumentaţie oficială faptul că „este nevoie de acces la comunicaţiile cifrate pentru a zădărnicii activităţile celor Patru Cavaleri ai Apocalipsei Internetului: crima organizată, traficanţii de droguri, pedofilii şi teroriştii" (David J. Lounday). Obiectivul FBI, al CIA, al NSA şi al tuturor organismelor care au rolul de a reprima criminalitatea în SUA şi în alte ţări este de a monitoriza utilizarea instrumentelor de codificare a informaţiilor care circulă prin toate reţele de comunicații existente.

În cadrul unei audieri, la data de 09 iulie 1997, în faţa Senatului, Louis Freeh, fost director al FBI, declara că tehnologia criptării şi folosirea ei necontrolată reprezintă un mare pericol pentru siguranţa naţională. În acest context, sublinia şi necesitatea includerii în legislaţia aferentă a prevederii obligatorii pentru producătorii din domeniu, de a introduce în structura departamentelor tehnice de criptare anumite caracteristici care să permită organelor de aplicare a legii decriptarea unor mesaje codificate, în baza unei autorizaţii emise de organele judiciare.

Pentru mulți oameni, faptul că autorităţile ar dori să aibă acces la cheile de criptare reprezintă un motiv de îngrijorare. Ei consideră, și pe bună dreptate, că monitorizarea guvernamentală strictă asupra criptografiei ar putea reprezenta un pericol pentru libertăţile civile și protecția vieții private, dacă este reglementată în aşa fel încât autorităţile să aibă acces la toate datele personale ale oricui, la fișele medicale, la mesajele transmise prin e-mail etc.

Într-un astfel de context, **evoluția prin câștig accelerat** este singura constantă a domeniului. Ca atare, cel mai bun lucru pe care îl putem face este să privim înapoi în istoria criptologiei şi să medităm la ce a rămas din cifrurile considerate anterior „impenetrabile". În cadrul luptei nesfârşite dintre criptografi şi criptanalişti, barierele ridicate de unii au fost, până la urmă, întotdeauna depăşite de ceilalţi.

Poate că într-o bună zi complexitatea factorizării numerelor foarte mari, fizica cuantică şi teoria haosului vor părea la fel de simple viitorilor spărgători de coduri, precum ne pare nouă permutarea lui Cezar.

Date fiind toate cele de mai sus, merită să ne punem întrebarea:
au fost atinse limitele ingeniozităţii umane în domeniul păstrării secretelor ?
Singurul răspuns de bun-simţ este că nu.
Câtă vreme vor exista oameni care au secrete de păstrat
şi alţi oameni care vor să le cunoască,
vor fi la mare preţ acei specialişti remarcabili care prin definiție
sunt condamnați sa lucreze în anonimatul binecuvântat al profesiei:
criptologii.
Cursa "înarmărilor cu cifruri", care se întinde de-a lungul mileniilor
şi care ne-a dus de la sisteme simple la paradoxurile fizicii moderne,
nu dă semne că ar avea sfârșire.

Gen.br. (r) **Vasile MAIEREAN**

BIBLIOGRAFIE SELECTIVĂ

1. Kahn, David - The Codebreakers, Editura Schribner, New York ,1996.
2. Newton, David - Enciclopedia of Criptology, Editura ABC - Clio, 1997.
3. Pincock, Stephen și Frary, Mark - Coduri. O istorie a comunicării secrete, Editura RAO, București, 2007.
4. Maierean Vasile și Dulciu, Dan - O istorie a criptologiei românești, Editura RAO, București, 2010 .
5. James Bamford, The Puzzle Palace: a Report on America's Most Secret Agency, Editura Penguin Books, 1983.
6. Tim Weiner, CIA o istorie secretă, Editura Litera Internațional, București, 2009.
7. Mills, James, The Under Ground Empire, Where Crime and Governments Embrance, Editura Doubleday&Company, New York, 1986.